

"Phishing" Schemes



One of the newest fraud schemes is called "phishing" and involves sending out thousands of e-mails fishing for personal information that is later used to commit identity theft. These e-mails either take you to a counterfeit site or install a keyboard logger when you click on the link. Either way, the thief then captures your personal information.

We have taken a number of these reports from West Linn victims. One of these victims had his account accessed within 20 minutes after submitting his information.

The "phishing" e-mails all share some common elements:

1. They will be addressed to "dear account holder" or something similar. If this was your bank or a business you deal with they will probably know your name.
2. There will be some reason why you need to respond. They will tell you they noticed unusual recent activity or just performed an audit of your account.
3. There will be some statement of urgency, often that your account will be frozen if you do not respond immediately.

For additional information on "phishing" and how to protect yourself check out this excellent link:

<http://www.microsoft.com/athome/security/email/phishing/video1.msp>

- [Police](#)

Source URL (retrieved on 2010-05-27 20:11): <http://westlinnoregon.gov/police/phishing-schemes>